INITIAL PERMUTATION: SIMPLE BIT ARRANGEMENT

IP always rearranges bit positions; it does not alter bit values

DES | DECRYPTION

IDEA: Select the input bits in the order stated by the IP table.

1 Begin with an 8-bit teaching example

1	2	3	4	5	6	7	8
1	0	1	1	0	0	1	0

2 Apply this miniature IP rule

[2, 4, 6, 8, 1, 3, 5, 7]

RESULT

10110010 → 01001101

Remember: IP moves positions. It does NOT use XOR or the secret key.

ACTUAL DES: APPLY IP TO THE CIPHERTEXT

The ciphertext is permuted first - before beginning Round 1

1 Start with the 64-bit encrypted block

CIPHERTEXT / C

85E813540F0AB405

2 Apply the fixed standard DES IP table

IP positions: 58, 50, 42, 34, 26, 18, 10, 2, ...



64-BIT RESULT

IP(C) = 0A4CD99543423234

This output is the starting block for the 16 decryption rounds.

SPLIT INTO LEFT AND RIGHT HALVES

After the initial permutation, create two 32-bit pieces

IP(C) = 0A4CD99543423234

FIRST 32 BITS: L0

0A4CD995

LAST 32 BITS: R0

43423234

DECRYPTION ROUND 1

Send R0 = 43423234 into F(R0, K16).

Each half has 8 hexadecimal digits = 32 bits.